UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,691	03/31/2004	Dennis M. O'Connor	80107.113US1	7241

7590 05/02/2007

LeMoine Patent Services, PLLC
c/o PortfolioIP
P.O. Box 52050
Minneapolis, MN 55402

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
05/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/814,691	O'CONNOR, DENNIS M.	
	Examiner	Art Unit	
	Oscar A. Louie	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 03/31/2004. Claims 1-26 are pending and have been considered as follows.

1. Claim 15 is rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for a processor comprising circuitry to differentiate between non-secure process having page tables in non-secure memory, secure processes capable of having page tables in non-secure memory or secure memory, and safer secure processes having page tables in secure memory, does not reasonably provide enablement for using a single definition for creating a number of objects. The apparatus in this claim consists of a single element: "circuitry to differentiate between non-secure process having page tables in non-secure memory, secure processes capable of having page tables in non-secure memory or secure memory, and safer secure processes having page tables in secure memory," and thus is interpreted as a single means claim under MPEP 2164.08(a).

"A single means claim, i.e., where a means recitation does not appear in combination with another recited element of means, is subject to an undue breadth rejection under 35 U.S.C. 112, first paragraph. In re Hyatt, 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983) (A single means claim which covered every conceivable means for achieving the stated purpose was held nonenabling for the scope of the claim because the specification disclosed at most only

those means known to the inventor.). When claims depend on a recited property, a fact situation comparable to Hyatt is possible, where the claim covers every conceivable structure (means) for achieving the stated property (result) while the specification discloses at most only those known to the inventor."

Drawings

2. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because informal (i.e. hand written) drawings are non-acceptable. Drawings for figures 1-7 are informal. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6, 8-10, & 13-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Sibert (US-7124170-B1).

Claim 1:

Sibert discloses a processor comprising,

- "a mechanism to identify memory as secure memory accessible by secure processes, and to identify non-secure memory accessible by both secure and non-secure processes" (i.e. "processor security registers 132 can be used to indicate which internal resources permit or do not permit such external access") [column 6 lines 53-55].
- "a security enforcement mechanism to allow page tables for the non-secure processes to be stored in secure memory" (i.e. "In other embodiments, external bus 104 may also be designed to support input addressing, so that external devices (including other processors) can initiate "direct memory access" (DMA) to the internal resources, memory, and/or other components of SPU 100") [column 6 lines 48-53].

Claim 2:

Sibert discloses a processor as in Claim 1 above further comprising,

- "the processor can operate in a secure mode and in a non-secure mode" (i.e. "FIG. 3 shows software running on SPU 100 that includes both protection-critical software 202 and other software 201") [column 6 lines 58-59].
- "the security enforcement mechanism allows page table walks for non-secure processes while in non-secure mode" (i.e. "That is, external bus 104 provides output-only addressing, but can transfer data for both input and output purposes") [column 6 lines 46-48].

Claim 3:

Sibert discloses a processor as in Claim 1 above further comprising,

- "the security enforcement mechanism includes page table walk hardware capable of walking page tables in secure memory in response to architecture events caused by non-secure processes" (i.e. "In such embodiments, processor security registers 132 can be used to indicate which internal resources permit or do not permit such external access") [column 6 lines 53-55].

Claim 4:

Sibert discloses a processor as in Claim 1 above further comprising,

- "the security enforcement mechanism includes circuits to differentiate between program generated memory accesses and architecture generated memory accesses, and to block program generated memory access from accessing secure memory" (i.e. "In such embodiments, processor security registers 132 can be used to indicate which internal resources permit or do not permit such external access") [column 6 lines 53-55].

Claim 5:

Sibert discloses a processor as in Claim 1 above further comprising,

- "a configurable memory management unit capable of requiring non-secure process to access secure memory when performing page table walks" (i.e. "In other embodiments, external bus 104 may also be designed to support input addressing, so that external devices (including other processors) can initiate "direct memory access" (DMA) to the internal resources, memory, and/or other components of SPU 100") [column 6 lines 48-53].

Claim 6:

Sibert discloses a processor as in Claim 1 above further comprising,

- "virtual address translation hardware to perform virtual address translation for non-secure processes via page tables in secure memory" (i.e. "Such dual decoding permits SPU monitor 203 to use a single address mapping (mapping some logical address to the physical page or pages where all control registers are present compactly) for system control purposes") [column 14 lines 46-49].

Claim 8:

Sibert discloses a processor as in Claim 1 above further comprising,

- "a control register to specify whether page tables for non-secure processes are kept in secure memory or nonsecure memory" (i.e. "In such embodiments, processor security registers 132 can be used to indicate which internal resources permit or do not permit such external access") [column 6 lines 53-55].

Claim 9:

Sibert discloses a processor as in Claim 1 above further comprising,

- "page table walk hardware capable of accessing secure memory on behalf of non-secure processes" (i.e. "In other embodiments, external bus 104 may also be designed to support input addressing, so that external devices (including other processors) can initiate "direct memory access" (DMA) to the internal resources, memory, and/or other components of SPU 100") [column 6 lines 48-53].

Claim 10:

Sibert discloses a processor comprising,

- "an apparatus to differentiate between hardware generated memory accesses and software generated memory accesses" (i.e. "memory management unit 131, which is used by monitor 203 to isolate memory regions accessible to different software modules. Memory management unit 131 can employ a variety of familiar mechanisms to effect such isolation, including paging, page protection, segmentation, segment limits, protection domains, capabilities, storage keys, and/or other techniques") [column 7 lines 55-62].
- "to grant secure memory access to hardware generated memory accesses" (i.e. "the translation tables are kept in internal memory 102 in order to guarantee their integrity and to ensure that only monitor 203, and specific authorized hardware functions (e.g., the MMU) can manipulate them") [column 8 lines 1-4].

Claim 13:

Sibert discloses a processor as in Claim 10 above further comprising,

- "the hardware generated memory accesses are the result of architecture events" (i.e. "the translation tables are kept in internal memory 102 in order to guarantee their integrity and to ensure that only monitor 203, and specific authorized hardware functions (e.g., the MMU) can manipulate them") [column 8 lines 1-4].

Claim 14:

Sibert discloses a processor as in Claim 13 above further comprising,

- "the architecture events result in a page table walk for a non-secure process" (i.e. "the translation tables are kept in internal memory 102 in order to guarantee their integrity and to ensure that only monitor 203, and specific authorized hardware functions (e.g., the MMU) can manipulate them") [column 8 lines 1-4].

Claim 15:

Sibert discloses a processor comprising,

- "circuitry to differentiate between non-secure process having page tables in non-secure memory, secure processes capable of having page tables in non-secure memory or secure memory, and safer secure processes having page tables in secure memory" (i.e. "Monitor 203 may use protection facilities (e.g., a memory management unit (MMU) that provides independent control for access to different pages and/or segments of memory) already present in conventional, off-the-shelf processors (such as those conforming to the INTEL.RTM. IA-32, ARM, MIPS, or SPARC architectures), to effect the desired isolation") [column 7 lines 13-20].

Claim 16:

Sibert discloses a processor as in Claim 15 above further comprising,

- "the circuitry comprises a memory management unit" (i.e. "a memory management unit (MMU)") [column 7 lines 14-15].

Claim 17:

Sibert discloses a processor as in Claim 16 above further comprising,

- "the memory management unit comprises a control register to prevent the processor from using non-secure memory when performing a page table walk for a secure process" (i.e. "a memory management unit (MMU) that provides independent control for access to different pages and/or segments of memory)") [column 7 lines 14-16].

Claim 18:

Sibert discloses a processor as in Claim 15 above further comprising,

- "page table walk hardware to perform page table walks" (i.e. "modules will typically be resident in separate memory spaces and have access to memory spaces controlled by monitor 203 so that they are effectively isolated from each other") [column 7 lines 5-8].

Claim 19:

Sibert discloses a processor as in Claim 18 above further comprising,

- "the processor can operate in a secure mode or non-secure mode" (i.e. "FIG. 3 shows software running on SPU 100 that includes both protection-critical software 202 and other software 201") [column 6 lines 58-59].
- "the page table walk hardware can perform page table walks without changing the mode in which the processor operates" (i.e. "Software modules will typically be resident in separate memory spaces and have access to memory spaces controlled by monitor 203 so that they are effectively isolated from each other") [column 7 lines 5-8].

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 7, 11, & 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sibert (US-7124170-B1) in view of Mahon et al (US-4809160-A).

Claim 7:

Sibert discloses a processor as in Claim 1 above but does not disclose,

- "a translation look-aside buffer (TLB), wherein the security enforcement mechanism allows a secure memory access after a TLB miss"

however, Mahon et al do disclose,

- "The Target Register 70 as shown in FIG. 3 contains the return address in Address Location 300 with the original, lower privilege level stored in two lower order bits 310. The TLB 30 then checks the access rights of the calling instruction as will be described shortly to determine if execute access is permitted" [column 3 lines 41-46].

Therefore, it would have been obvious for one having ordinary skill in the art at the time of the applicant's invention to include, "a translation look-aside buffer (TLB), wherein the security enforcement mechanism allows a secure memory access after a TLB miss," in the invention as disclosed by Sibert since a translation look-aside buffer would be commonly used to check the access rights of instructions particularly when dealing with memory access.

Claim 11:

Sibert discloses a processor as in Claim 10 above but does not disclose,

- "the hardware generated memory accesses are the result of a translation look-aside buffer (TLB) miss"

however, Mahon et al do disclose,

- "The Instruction Unit 20 seeks this higher privileged routine by addressing the Translation Lookaside Buffer (TLB) 30 via the Virtual Address Bus 35 to determine the location in Physical Memory 40 containing an appropriate entry point of a gateway instruction" [column 3 lines 22-27].

Therefore, it would have been obvious for one having ordinary skill in the art at the time of the applicant's invention to include, "the hardware generated memory accesses are the result of a translation look-aside buffer (TLB) miss," in the invention as disclosed by Sibert since a translation look-aside buffer miss indicates that no virtual address is mapped to a physical address, which would be implied since hardware generated memory accesses would have direct memory access.

Claim 12:

Sibert and Mahon et al disclose a processor as in Claim 11 above but Sibert does not explicitly disclose,

- "hardware generated memory accesses may be caused by secure or non-secure processes"

however, Mahon et al do disclose,

- "The actual security protection by the TLB 30 is the same for "normal" instructions as for accessing a gateway instruction, and is performed with a granularity of an entire page of virtual memory" [column 4 lines 7-10].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "hardware generated memory accesses may be caused by secure or non-secure processes," in the invention as disclosed by Sibert since it is normal for hardware generated memory accesses to occur regardless of the process security.

7. Claims 20-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mahon et al (US-4809160-A) in view of Sibert (US-7124170-B1).

Claim 20:

Mahon et al disclose a method comprising,

- "determining if a translation look-aside buffer (TLB) miss has occurred" (i.e. "The Instruction Unit 20 seeks this higher privileged routine by addressing the Translation Lookaside Buffer (TLB) 30 via the Virtual Address Bus 35 to determine the location in Physical Memory 40 containing an appropriate entry point of a gateway instruction" [column 3 lines 22-27].
- "if the current process page table is in secure memory, performing a page table walk in secure memory" (i.e. "If execute access is allowed by the TLB 30, and no delayed taken branch is pending, the gateway instruction resaves the actual privilege level of the calling routine in the two low-order bits of Target Register 70 (to rule out forgery by the calling routine), and raises the privilege level of the calling routine to the privilege level

specified within the page type field 412 of the TLB entry for the page containing the gateway instruction, and a target address for branching to a called routine is calculated in either the Instruction Unit 20 or the Execution Unit 60, as appropriate") [column 3 lines 50-61].

but Mahon et al do not disclose,

- "determining if a current process page table is in secure or non-secure memory"

however, Sibert does disclose,

- "In such embodiments, processor security registers 132 can be used to indicate which internal resources permit or do not permit such external access" [column 6 lines 53-55].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "determining if a current process page table is in secure or non-secure memory," in the invention as disclosed by Mahon et al for the purposes of determining whether access is to be permitted to each type of memory.

Claim 21:

Mahon et al and Sibert disclose a method as in Claim 20 above, Mahon et al further disclose,

- "the page table walk is performed for a secure process" (i.e. "The actual security protection by the TLB 30 is the same for "normal" instructions as for accessing a gateway instruction, and is performed with a granularity of an entire page of virtual memory") [column 4 lines 7-10].

Claim 22:

Mahon et al and Sibert disclose a method as in Claim 20 above, Mahon et al further disclose,

- "the page table walk is performed for a nonsecure process" (i.e. "The actual security protection by the TLB 30 is the same for "normal" instructions as for accessing a gateway instruction, and is performed with a granularity of an entire page of virtual memory") [column 4 lines 7-10].

Claim 23:

Mahon et al and Sibert disclose a method as in Claim 20 above but Mahon et al do not explicitly disclose,

- "if the current process page table is in non-secure memory, performing the page table walk in non-secure memory"

however, Sibert does disclose,

- "a "non-critical only" attribute for the page table it designates, the attribute indicating that the page base addresses in level-two page table 305 can designate only "non-critical" memory regions" [column 11 lines 30-33].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "if the current process page table is in non-secure memory, performing the page table walk in non-secure memory," in the invention as disclosed by Mahon et al for the purposes of allowing regular non-secure page table operations.

8. Claims 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mel et al ("Tablet: Personal Computer of the Year 2000") in view of Sibert (US-7124170-B1).

Claim 24:

Mel et al disclose an electronic system comprising,

- "a plurality of antennas" (i.e. "The main use for the cellular link will be to communicate with other computers and the people using them") [page 642].
- "an amplifier coupled to at least one of the plurality of antennas to amplify communications signals" (i.e. "The main use for the cellular link will be to communicate with other computers and the people using them") [page 642].
- "a processor coupled to the amplifier" (i.e. "the processor") [page 642].

but Mel et al do not disclose,

- "memory that can be partitioned by the processor into secure memory accessible by secure processes and non-secure memory accessible by secure or nonsecure processes; wherein the processor includes a security enforcement mechanism to allow page tables for non-secure processes to be stored in secure memory"

however, Sibert does disclose,

- "Both software 201 and software 202 may comprise many modules, only some of which may be resident in secure memory 102 at any particular time. Software modules will typically be resident in separate memory spaces and have access to memory spaces controlled by monitor 203 so that they are effectively isolated from each other" [column 7 lines 2-8].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "memory that can be partitioned by the processor into secure memory accessible by secure processes and non-secure memory accessible by secure or nonsecure processes; wherein the processor includes a security enforcement mechanism to allow page tables for non-secure processes to be stored in secure memory," in the invention as disclosed by Mel et al for the purposes of having securely isolated memory spaces.

Claim 25:

Mel et al and Sibert disclose an electronic system as in Claim 24 above, but Mel et al do not explicitly disclose,

- "the processor can operate in a secure mode and in a non-secure mode"
- "the security enforcement mechanism allows page table walks for non-secure processes while in non-secure mode"

however, Sibert does respectively disclose ,

- "FIG. 3 shows software running on SPU 100 that includes both protection-critical software 202 and other software 201" [column 6 lines 58-59].
- "a "non-critical only" attribute for the page table it designates, the attribute indicating that the page base addresses in level-two page table 305 can designate only "non-critical" memory regions" [column 11 lines 30-33].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "the processor can operate in a secure mode and in a non-secure mode" and "the security enforcement mechanism allows page table walks for non-secure processes while in non-secure mode," in the invention as disclosed by Mel et al for the purposes of having a versatile system that can operate and handle both secure and non-secure operations.

Claim 26:

Mel et al and Sibert disclose an electronic system as in Claim 24 above but Mel et al do not disclose,

- "the security enforcement mechanism includes page table walk hardware capable of walking page tables in secure memory in response architecture events caused by non-secure processes"

however, Sibert does disclose,

- "In such an embodiment, processor security registers 132 can be used to designate internal memory as critical, but external memory 105 (accessed by external bus 104) as non-critical" [column 11 lines 34-37].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "the security enforcement mechanism includes page table walk hardware capable of walking page tables in secure memory in response architecture events caused by non-secure processes," in the invention as disclosed by Mel et al for the purposes of improving efficiency by permitting non-secure access in secure memory when necessary.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Strongin et al (US-6854039-B1) – overall elements and memory management unit

b. Ikeda (US-4954944-A) – cache control

c. Easter et al (US-5530749-A) – secure computer chip

d. Hale et al (US-6564317-B1) – lockable nonvolatile memory

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Myhre, can be reached at 571-270-1065. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
04/25/2007

James Myhre
Supervisory Patent Examiner

KIEU VU
PRIMARY EXAMINER